Remarks

Interview Summary

The Applicants sincerely appreciate the courtesy extended by Examiners Coggins and Haq for participating in the interview of August 6, 2003 with the undersigned. The interview summary mailed August 12, 2003 appears accurate.

Declaration of Inventors

The declaration of the inventors has been objected to as not referring to any amendments made between filing and the date of signature of the declaration. Since no such amendments were made this appears moot. If the Examiner believes this is still needed in view of the complete absence of any intervening amendments, then a substitute declaration will be provided.

Cancellation of Prior Claims

The Applicants' have elected to cancel the prior claims. This is done without prejudice to or acquiescence in the rejections made. The new claims presented are believed to clarify and demonstrate the non-obvious nature of the invention while also avoiding the concerns expressed in the Office Action.

Discussion of Rejections Given in Office Action and Applied Prior Art

The applied reference in making the rejections under §103 of the Patent Acts is U.S. Patent No. 5,883,810 to Franklin et al. (hereinafter referred to as the Franklin Patent for convenience). The Franklin Patent teaches a different approach to purchasing over the internet and does not prevent fraudulent use of the account, instead it merely limits the exposure to a single or few incidents as described therein.

Franklin still transmits via the internet a pseudo-card number that is also described as a transaction number. The pseudo-card number is described as a proxy card number for use of an undisclosed account number that the account holder does not know.

The essence and proper interpretation of Franklin is that it is merely issuing short term charge card numbers. These short term charge card numbers are used once or a few times and are indicated to be capable of additional security by indicating the merchant and amount.

In all implementations described in the Franklin Patent the limited use card number or transaction number *are transmitted via the internet from the issuing bank to the customer*. This renders the card number subject to interception and misuse.

The same number transmitted from the bank to the customer is also again being subjected to inception and misuse because it is further transmitted via the internet from the customer to the merchant. The number being transmitted from the bank to the customer and from the customer onto the internet provide fraud enablement. The number is a "proxy charge card number". An astute criminal can intercept this number and use it quickly in another transaction. For example, the criminal may intercept the proxy card number and then effectuate a charge before the rightful customer completes his or her shopping and uses the proxy number to make a charge.

Franklin explains this itself at Col. 2, lines 56-67. To quote a portion of this passage appropriate at this point in the consideration of this reference:

> The online commerce system substantially reduces the value of a stolen number since the transaction number that is transmitted over the Internet (or other network) is only a proxy number for a single purchase.

Although Franklin incorrectly indicates that value is reduced. The full value authorized in advance by the bank is at risk. Possibly the reference is that the whole credit limit of the account is not available. However, this could very well be the case with the Franklin approach. The person who has

decided to pay off another account or purchase on object for the full credit value would be authorized under the Franklin scheme and the fraud-enabling proxy number is transmitted over the internet for possible interception at two stages and at unknown transmission nodes therebetween.

Although Franklin purports to solve the problem, it does not do so. Instead, it reduces risk and severely inconveniences the customer. In advance of every shopping attempt the customer must get an authorized proxy card number that may only be good for a period of 30 minutes. Thus, the customer may be left repeatedly going back to the bank and seeking new proxy card numbers before even one product is successfully purchased. This is quite simply impractical and will not be tolerated by most customers. This may be one of the reason the single transaction number approach has not be widely received by the customer population.

The Applicant's claimed and novel methodology does not require ANY EXPOSURE OF ANY FRAUD-ENABLING INFORMATION VIA THE INTERNET. It does this by a technique that is a significant and patentable development and discovery and provides surprising results in that internet purchasing can be truly rendered secure. As the Examiner's indicated many attempts have been made to provide secure purchasing over the internet.

This invention accomplishes what the others have failed to do in a procedure that is relatively easy for the customer, bank and merchant to implement.

Discussion of New Claims

Claim 28 provides a method that includes the step of communicating between customer and merchant computers without providing fraud enabling information. A transaction number is assembled with the order information. This can be done by either the merchant or customer as indicated respectively starting at p. 58, line 1 and p.75, line 8, and possibly other locations in the specification as originally filed.

The transaction number cannot be used by either the merchant or anyone else to effect a fraudulent transaction. At this stage of the novel methods the transaction number merely identifies an order set up in whole or in part between the customer and merchant. Confirmation by the customer using a identification inquiry is needed for the transaction identification to take life and become useful. This must be contrasted by the approach taken by the Franklin Patent which communicates a fully enabled proxy card number which appears to all except the processing bank as a valid charge card number.

As claim 28 recites, the bank computer and customer then perform by communicating via the internet to provide a sufficient customer identification inquiry. If this inquiry and all other factors needed for authorization of a purchase transaction are acceptable then the merchant is given assurance of payment.

In the Applicant's recited method the unusable transaction number which results from the customer/merchant exchange then is tied to one particular transaction between the that merchant and that customer. To the Applicants' knowledge no other approach has this combination of features and no other approach provides truly secure internet purchasing and payment transactions. Encryption techniques merely make fraud more difficult, but history has proven that almost any encryption technique may be broken.

To the contrary, in the Franklin Patent, the customer authentication is done prior to releasing the proxy charge card number. The proxy charge card number is then *transmitted over the internet to the user*. This is done in a session where a PIN is likely used and is also capable of interception. Once the proxy card number is sent over the internet it can be used by anyone until the prescribed time expires or other conditions are met. The prescribed time indicated as preferred is 30 minutes to 2 hours. This is more

than ample time to allow a scheming internet thief who is ready to intercept the number and effectuate a fraudulent charge. Thus, the Franklin Patent has great emphasis on keeping the time period very short. This necessarily has a dramatic effect on the convenience and consumer acceptance of this approach.

Franklin does not solve the problem he merely shortens the time during which commission of the crime may occur and reduces the possible number of times the fraud can take place. At best, information about a merchant and item is included. But an internet thief can still intercept this information and thus obtain the previously chosen article. This is indicated in the Franklin Patent at many places, such as quoted above. At Col. 4, line 53, a sentence reads:

> The issuing bank 26 issues the transaction number to the customer to use as a proxy for the real customer account number. The transaction number resembles a real account number. In the case of a credit card for example, the transaction number and real customer account number are both 16-digit, mod 10, number identically formatted with four spaced sets of 4-digits. To the customer (and every other participant in the transaction), the transaction number appears to be a *valid credit card number*. (emphasis added)

In fact these proxy numbers are valid credit card numbers waiting to be used. In some embodiments, the numbers are limited to only one use. In other described embodiments the proxy cards numbers are multiple use but limited in time. These are simply credit card numbers sent over the internet for possible interception with a budget that may be limited, a time utilization period that is limited, and in rare cases limitation to a merchant and goods.

Claim 28 is non-obvious over the Franklin Patent by reciting that the communicating and assembling steps are performed without communicating a customer account number or similar customer account identification. The proxy card number is a customer account number limited in use. Thus the Franklin Patent does not render the combination of claim 28 obvious under §103 of the Patent Acts.

The language of claim 28 also recites that the account identification may not be used to make fraudulent transactions. Clearly, the Franklin Patent technology will allow interception and fraudulent transactions to occur if the perpetrator is ready and able since all the information is placed into the public in an instantly accessible form on the internet.

Claim 28 is also non-obvious under §103 because it recites a combination of method steps which include assigning a transaction identifier

that is not useful for making other transactions against the customer account. The customer and merchant initiate the transaction identifier and it is communicated to the bank and tied definitively to that one transaction and to a customer that meets the authentication or verification parameters. No such provision is made in the Franklin Patent and it does not render the novel combination obvious.

Claim 28 further recites communicating between the customer computer and bank computer via the internet to provide authorization of a purchase transaction based upon said order information and including at least said transaction identification and merchant identification. Although the Franklin Patent speaks in terms of optionally using information about merchant and cost; this is done in a different use. The Franklin Patent approach does not after the proxy card number is issued limit who is able to use the card. This is true even though it may be limited to a single use. A single fraudulent use of a millionaire's "secure proxy card" by a internet fraud artist may still represent a substantial loss to the customer, card company or merchant.

Claim 29 is patentable because of the reasons given above for main claim 28 and because it recites the non-obvious step of the customer assembling the transaction identifier. Conversely, claim 30 recites that the

merchant assigns the transaction identifier. Both are indicated in the specification as explained above.

Claims 31-37 are based on main claim 28 and allowable for the same reasons. Each has differing limitations as to the verification or authentication fields used either singly or in plural and whether they change with each customer transaction or with each transaction. Claims 31-37 are believed allowable.

Claims 38-40 are also based on main claim 28 and further recite an identification inquiry between the bank and merchant. The Franklin Patent does not teach the combination of method steps defined by each such claim and does not render any of these claims obvious within the meaning and proper interpretation of §103 of the Patent Acts.

Group B of the claims includes new claim numbers 41-53. Many or all of the arguments given above are applicable to these claims as well and render the claims non-obvious under §103. Main claim 41 is similar to claim 28 with an added feature that the communicating between the customer computer and bank computers includes cost information. Thus the arguments given herein are applicable to both Groups A and B, except as noted and other language may vary.

The novel and non-obvious methods defined by the claims pending in this application are believed to fully meet the requirements for patentability and favorable action thereon is respectfully requested.

Respectfully Submitted,

Date: March 12, 2004

Randy A. Gregory, Reg. No. 30,386